



# UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,002	07/05/2001	Mark J. McArdle	002114.P020	5144
28875	7590	10/26/2005	EXAMINER	
Zilka-Kotab, PC P.O. BOX 721120 SAN JOSE, CA 95172-1120			PWU, JEFFREY C	
			ART UNIT	PAPER NUMBER
			2143	
DATE MAILED: 10/26/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/900,002

Applicant(s)

MCARDLE ET AL

Examiner

Jeffrey C. Pwu

Art Unit

2143

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date ____. | 6) <input type="checkbox"/> Other: ____.  |

**DETAILED ACTION**

1. The final rejection of claims 1-29 over **Ginter** et al. is hereby withdrawn in view of applicants' appeal brief filed 8/3/2005 and newly discovered prior art. Any inconvenience is regretted.

**Claim Rejections - 35 USC § 112**

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1 is vague and indefinite because it is unclear of the limitation "detecting a network access request from an application", it is unclear how to request an application based on a detection from a network access or when based on a network access, how to execute, detect, and/or request an application to restrict a network access?

4. Claim 20 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is vague and indefinite because it is unclear what data or what action is contained in the limitation "containing data specifying an action to performed if the application identified by the application identifier field attempts access to the entity identified by the network identifier field and the access is not allowed."

**Claim Rejections - 35 USC § 102**

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-29 are rejected under 35 U.S.C. 102(e) as being anticipated by **Kahn** et al.

(U.S. 6,135,646). Hereinafter **Kahn**.

**Kahn** teaches claims:

1. A computerized method for restricting network access by applications comprising:

- detecting a network access request from an application; (the examiner interprets the limitation as follows: **Kahn** discloses a tracking system 46, detecting and tracking examination of a registration system 40 of registered rights – col.8, lines 6-40 and “an access mechanism for applying terms and conditions for access to each of the digital objects, the mechanism including information about the terms and conditions, and the mechanism being arranged to make the information about terms and conditions available to a user in connection with a request for access to one of the digital objects, to enable the user to indicate assent to the terms and conditions, and to permit access to the user only upon the user indicating assent to the terms and conditions.” – claim 10)
- examining an application policy file (col.7, lines 50-60, col.8, lines 6-35 and claims 1 and 10) to determine if the application is authorized to access the network by comparing an identifier for

the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network; and (Claims 1 & 10: “digital objects, each of the digital objects comprising one or more sequences of structured data or sets of such sequences, each of the sequences or sets of sequences incorporating a work or a portion of a work or other digital information in which a party has rights or interests, or in which there is value, each of the sequences or sets of sequences being structured in a way that is interpretable by one or more of the computational facilities in the network, each of the digital objects including an identifier that uniquely identifies the digital object within the network and persists, with respect to the digital object, over a period of time that is at least as long as the existence of the digital object, an administrative mechanism that (a) is distributed among the computational facilities, (b) assures the uniqueness and persistence of the identifiers over a time period that is at least as long as the existence of the digital objects, and (c) distributes state information that includes the identifiers among computational facilities by an algorithmic process for managing the uniqueness and persistence of the identifiers, at least some of the digital objects including other structured data which is useful in processing the digital objects, including managing access to them, and a resolution mechanism that accepts unique identifiers as input and resolves each of the identifiers to state information that denotes a computational facility or other digital object that contains the digital object associated with the unique identifier; an access mechanism for applying terms and conditions for access to each of the digital objects, the mechanism including information about the terms and conditions, and the mechanism being arranged to make the information about terms and conditions available to a user in connection with a request for access to one of the digital objects, to enable the user to

Art Unit: 2143

indicate assent to the terms and conditions, and to permit access to the user only upon the user indicating assent to the terms and conditions.”)

- blocking access to the network if the application is not authorized to access the network. (col.2, lines 17-47 and col.3, lines 14-26)

2. The method of claim 1 further comprising: determining a network resource requested by the application; examining the application policy file to determine if the application is authorized to access the network resource; and allowing access to the network resource if the application is authorized to access the network resource. (col.7, lines 50-60, col.8, lines 6-35 and claims 1 and 10)

3. The method of claim 1 further comprising: determining a type of network access requested by the application; examining the application policy file to determine if the application is authorized for the type of network access requested; and allowing the type of network access requested if the application is authorized for the type of network access requested. (col.7, lines 50-60, col.8, lines 6-35 and **Kahn** - claims 1 and 10)

4. The method of claim 1 further comprising: updating the application policy file and re-evaluating applications currently executing against the updated policy file. ((col.7, lines 50-60, col.8, lines 6-35 and **Kahn** - claims 1 and 10)

5. The method of claim 1, wherein the application identifier is in the network access request.

(col.6, lines 22-25)

6. The method of claim 1, wherein the method is performed on a client computer on which the application is executing. (14)

7. A computer-readable medium having executable instruction to cause a computer to perform a method comprising: detecting a network access request from an application; examining an application policy file to determine if the application is authorized to access the network by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network; and blocking access to the network if the application is not authorized to access the network. (claim 7 is similarly rejected as in claim 1)

8. The computer-readable medium of claim 7, wherein the method further comprises: determining a network resource requested by the application; examining the application policy file to determine if the application is authorized to access the network resource; and allowing access to the network resource if the application is authorized to access the network resource. (claim 8 is similarly rejected as in claims 1-6)

9. The computer-readable medium of claim 7, wherein the method further comprises: determining a type of network access requested by the application; examining the application

Art Unit: 2143

policy file to determine if the application is authorized for the type of network access requested; and allowing the type of network access requested if the application is authorized for the type of network access requested. (claim 9 is similarly rejected as in claims 1-6)

10. The computer-readable medium of claim 7, wherein the method further comprises: updating the application policy file; and re-evaluating applications currently executing against the updated policy file. (claim 10 is similarly rejected as in claims 1-6)

11. The computer-readable medium of claim 7, wherein the application identifier is in the network access request. (claim 11 is similarly rejected as in claims 1-6)

12. A computer system comprising:

a processing unit; a memory coupled to the processing unit through a bus; a network interface coupled to the processing unit through the bus and further operable for coupling to a network; (42, 43, 34, 40, 41, 44 and 46) and an application policy process executed from the memory by the processing unit to cause the processing unit to detect a network access request from an application, to examine an application policy file to determine if the application is authorized to access the network by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network, and to block access to the network if the application is not authorized to access the network. (claim 12 is similarly rejected as in claim 1)



Art Unit: 2143

13. The computer system of claim 12, wherein the application policy process further causes the processing unit to determine a network resource requested by the application, to examine the application policy file to determine if the application is authorized to access the network resource, and to allow access to the network resource if the application is authorized to access the network resource. (claim 13 is similarly rejected as in claims 1-6)

14. The computer system of claim 12, wherein the application policy process further causes the processing unit to determine a type of network access requested by the application, to examine the application policy file to determine if the application is authorized for the type of network access requested, and to allow the type of network access requested if the application is authorized for the type of network access requested. (claim 14 is similarly rejected as in claims 1-6)

15. The computer system of claim 12, wherein the application policy process further causes the processing unit to update the application policy file, and to re-evaluate applications currently executing against the updated policy file. (col.7, lines 50-60, col.8, lines 6-35 and claims 1 and 10)

16. The computer system of claim 12, wherein the application identifier is in the network access request. (claim 16 is similarly rejected as in claims 1-6)

17. The computer system of claim 12, wherein the application is executed from the memory by the processing unit. (42, 43, 34, 40, 41, 44 and 46)

18. A computer-readable medium having stored thereon an application policy data structure comprising: an application identifier field containing data identifying an application that is authorized for installation on computer coupled to a network; a network identifier field containing data identifying a entity that is accessible by the application identified by the application identifier field; and an access flag field containing data specifying whether the application identified by the application identifier field is allowed access to the entity identified by the network identifier field. (col.7, lines 50-60, col.8, lines 6-35 and claims 1 and 10))

19. The computer-readable medium of claim 18 further comprising: an additional policy rule field containing data specifying whether the application identified by the application identifier field is allowed a particular type of access to the entity identified by the network identifier field. (col.7, lines 50-col.8, line 35)

21. The computer-readable medium of claim 18, wherein the entity is selected from the group consisting of a network and a network resource. (abstract)

22. The method of claim 5, wherein the application identifier is selected from the group consisting of a file name of the application and a path on the network. (col.7, lines 50-60, col.8, lines 6-35 and claims 1 and 10)

23. The method of claim 5, wherein a plurality of the application identifiers are associated with each application, and each of the application identifiers corresponds to a different network address assigned to the corresponding application. (col.7, lines 50-60, col.8, lines 6-35 and claims 1 and 10)

24. The method of claim 1, wherein each application entry in the application policy file comprises a set of access policy rules for one of a network and a network resource identified by a network identifier. (**Kahn** - claim 1)

25. The method of claim 24, wherein the network identifier is selected from the group consisting of a network address range and a Universal Naming Convention path. (“col. 24, line 34- “For retrieval purposes, the requesting system establishes a connection to the repository 766, which takes the form of a small set of transactions. The repository may examine the calling network address or the requesting system in order to determine if the repository is being inundated with requests from one system. If the repository determines that it is being bombarded, the repository may disconnect from the requesting system and refuse to accept additional requests for a period of time 768.”)

28. The method of claim 1 wherein the application policy file includes an application identifier, a network identifier, an access flag, additional policy rules, and at least one application entry. (col.7, lines 50-60, col.8, lines 6-35 and claims 1 and 10)

29. A computerized method for execution on a computer coupled to a network to restrict network access by an application executing on the computer, the method comprising:

- detecting a network request from the application, the request comprising at least one of an identifier and entity and a type of network access, wherein the entity is one of a network and a network resource; (col.7, lines 50-60, col.8, lines 6-35 and claims 1 and 10)
- examining an application policy file to determine if the application is authorized to access the entity by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network, wherein each application entry in the application policy file comprises a set of access policy rules for a network corresponding to a network identifier, the network identifier comprising at least one of a network address range and a Universal Naming Convention path, and wherein the application policy file further comprises an access flag having a null setting that is interpreted as one of allowing and disallowing all access to a network specified by the network identifier;
- blocking access to the entity if the application is not authorized to access the entity; and
- re-evaluating applications currently executing against any updated application policy file, wherein a plurality of the application identifiers are associated with each application, each application identifier corresponding to a different network address assigned to the corresponding application, and wherein each application identifier is one of a file name of the application and a path on the network. (46, tracking system, re-evaluating application identifiers; also see fig. 10 of Kahn)

**Response to Arguments**

7. Applicant's arguments with respect to claims 1-29 have been considered but are moot in view of the new ground(s) of rejection.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey C. Pwu whose telephone number is 571-272-6798.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Wiley can be reached on 571-272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



10/19/05

JEFFREY PWU  
EXAMINER